

مدیریت کلید در شبکه های حسگر بی سیم

شهرزاد فرهادپور^۱ رسول روستایی^۲

^۱ دانشجوی کارشناسی ارشد دانشگاه آزاد اسلامی واحد همدان

^۲ عضو هیئت علمی دانشگاه آزاد اسلامی واحد ملایر

چکیده:

پیشرفت های اخیر در تکنولوژی کامپیوتری الکترونیکی بستر مهمی را برای شبکه های WSN یا شبکه های سنسوری بی سیمی ایجاد کرده است. شبکه های سنسوری معمولاً شامل دستگاههای خودکار بسیار کوچک و ریزی هستند. هر دستگاه را یک گره های حسگری می نامند و دارای قدرت و باتری بخصوص است و با یک سنسور تعبیه شده در آن توانایی پردازش داده ها و ایجاد ارتباطات رادیویی در مسافت های کوتاه را دارند. در یک دستگاه سنسوری، گره های حسگر به شکل رانندومی در تمامی نواحی پخش می شوند تا داده های سنسوری را دریافت و جمع آوری کنند. یکی از مهمترین موضوع های موجود مسئله مدیریت کلیدی است که در بسیاری از تحقیقات و مطالعات مورد بررسی قرار گرفته است. مدیریت کلید به عنوان بخش اساسی یک ارتباط امن محسوب می شود پروتکل ارتباطی امن در شبکه، به سیستم مدیریت کلید موثر و مقاوم و امن بستگی دارد. از جمله ارتباطات بی سیم، شبکه های حسگر بی سیم می باشد. شبکه های حسگر بی سیم یک سیستم توزیع شده، خود مختار و خود سازمانده است که از تعداد زیادی گره های حسگر کوچک با عملیاتی که به انرژی کمی نیاز دارد تشکیل شده است. شبکه های حسگر بی سیم از اهمیت زیادی در علوم برخوردار است. از جمله کاربردهای مهم آنها نظارت و کنترل فرآیندهای صنعتی، نظارت بر سلامت دستگاهها، نظارت بر محیط و یا خانه، کاربردهای مراقبت از سلامتی، خانه های هوشمند و کنترل ترافیک می باشد.

کلید واژه: مدیریت کلید، شبکه، حسگر، بی سیم

مقدمه

شبکه های حسگر بی سیم از تعداد زیادی از گره های حسگر با قابلیت های حس کردن، ارتباط بی سیم و پردازش داده تشکیل شده است. این گره های حسگر به صورت مشارکتی وظایف حس پیچیده و جمع آوری داده و کار تلفیقی در یک حوزه خاص را انجام می دهند.

شبکه های حسگر بی سیم از موضوعات جدید و بسیار مهم در دانش روز پردازش و فناوری اطلاعات محسوب می شود که این شبکه گزینه مناسبی برای حالاتی است که ما به محیط هدایت شده دسترسی نداشته باشیم. این شبکه ها مستقل و خودگردان بوده و بدون دخالت انسان کار می کنند. شبکه های حسگر بی سیم، شبکه

هایی هستند که معمولاً برای نظارت و کنترل محیط های اطراف مورد استفاده قرار می گیرند (۱).

در ارتباط با شبکه های حسگر بی سیم یکی از مهمترین موضوع های موجود مسئله مدیریت کلیدی است که در بسیاری از تحقیقات و مطالعات مورد بررسی قرار گرفته است. سه نوع طرح و برنامه ی کلیدی کلی وجود دارند. طرح سرورهای قابل اعتماد، طرح خود تقویتی و طرح توزیع از قبل. طرح و راهبرد سرورهای قابل اعتماد بر اساس یک سرور قابل اعتماد و معتبر برای توافق های کلیدی بین دو گره است. به عنوان مثال Kerberos. این نوع طرح ها اغلب برای شبکه های حسگر مناسب نیستند. چرا که هیچ گونه زیر ساخت قابل اعتماد در شبکه های حسگری وجود ندارد. طرح های خود تقویتی شامل یک نوع آشکار سازی و مخفی سازی است. در این توافق کلیدی از یک گواهینامه ی کلیدی عمومی استفاده می کند. با این حال محاسبات محدود و منابع انرژی گره های حسگر اغلب استفاده از این محتوی الگوریتم کلید عمومی را غیر مطلوب می سازد.

همانند توافق کلیدی Hellman و RSA. نوع سوم طرح توافق کلیدی طرح توزیع از قبل است. در این طرح قبل از استفاده تمامی اطلاعات کلیدی بین گره های حسگر توزیع می شود. اگر ما بدانیم که کدام گره قبل از گسترش و استفاده در کدام قسمت است در این صورت کلید ها را می توان از قبل تصمیم گیری کرد. با این حال به علت رانندومی بودن و به کارگیری این سیستم ها شناسایی مجموعه ی دستگاه های محیط غیر قابل منطقی خواهد بود. تعداد زیادی از طرح های قبل از توزیع وجود دارند. یک روش غیر حرفه ای و آماتور این است که به تمامی گره ها این اجازه را بدهیم که یک شاه کلید داشته باشند.

هر کدام از این گره ها می توانند از این کلید های مخفی برای رسیدن به توافق کلیدی و سبک کلید جدید نیز استفاده کنند. این طرح نشان دهنده ی مقاومت و دوام شبکه ای مطلوب و دلخواه نیست. اگر یک گره به مخاطره بیافتد امنیت تمامی شبکه های دیگر نیز به مخاطره خواهد افتاد. برخی از مطالعات نشان داده اند که استفاده از شاه کلید ها در سخت افزارهای مقاوم در برابر مخفی سازی می تواند بسیار قوی عمل کند. اما این موضوع باعث افزایش قیمت و انرژی مصرفی هر حسگر خواهد شد.

علاوه بر این ها سخت افزارهای مقاوم در برابر مخفی سازی همیشه امن نیست. دیگر طرح قبل از توزیع به هر حسگر این اجازه